IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

Marc Joye

Application No.: 10/537,300

Filed: June 2, 2005

For: METHOD FOR SECURE INTEGER DIVISION OR MODULAR REDUCTION AGAINST HIDDEN CHANNEL ATTACKS

MAIL STOP AF

Group Art Unit: 2131

Examiner: Longbit Chai

Confirmation No.: 1466

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant requests review of the rejection of claims 1-8 set forth in the Office Action dated September 2, 2008 and maintained in the Advisory Action dated December 16, 2008. This Request is being filed with a Notice of Appeal. No additional amendments are being filed in response to the Office Action.

Rejection Under 35 U.S.C. § 102

Claims 1-8 are pending in this application. Claims 1, 2 and 5-8 stand rejected under 35 U.S.C. § 102(e) as anticipated by Drexler U.S. Patent Pub. No. 2003/0079139. Applicant respectfully traverses this rejection.

As set forth in MPEP § 2131, to anticipate a claim, the reference must teach every element of the claim. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987). The United States Court of Appeals for the Federal Circuit recently emphasized that "unless a reference discloses within the four corners of the document not only all of the limitations claimed but also all of the limitations arranged or combined in the same way as recited in the claim, it cannot be said to prove prior invention of the thing claimed and, thus, cannot anticipate under 35 U.S.C. § 102." *Net MoneyIN, Inc. v. VeriSign, Inc*, 545 F.3d 1359, 1371 (Fed. Cir. 2008) (emphasis added).

Applicant respectfully submits that this rejection does not meet the requirement because the Action does not establish that Drexler teaches every element of the claims arranged or combined in the same way as recited in the claims. For example, Applicant's claim 1 recites a cryptographic method during which an integer division of a type q = a div b and/or a modular reduction of a type r = a mod b is performed, where q is a quotient, a is a number containing m bits, b is a number containing n bits, with n less than or equal to m and b_{n-1} is non-zero, b_{n-1} being the most significant bit of the number b, comprising the steps of masking the number a by a random number ρ before performing the integer division and/or the modular reduction, and generating encrypted or decrypted data in accordance with a result of the division and/or modular reduction.

Exemplary embodiments encompassed by Applicant's claims are directed to a method of integer division or modular reduction secure against covert channel attacks, and in particular, differential attacks. Such methods can be implemented in electronic devices such as chip cards, for example. According to an exemplary embodiment, the number a can be masked by a random number ρ before performing the integer division and/or the modular reduction. With the number a being masked by a random number, the trace (for example, the energy consumption) left during the execution of the method is different at each execution, so that it is no longer possible to implement a differential covert channel attack. The random number ρ can be modified at each execution of the method, or simply after a predefined number of executions of the method.

Applicant respectfully submits that this same combination of features is neither disclosed nor suggested by Drexler. For example, paragraphs [0004] and [0007] in Drexler are cited for allegedly disclosing the claimed "cryptographic method during which an integer division of a type q = a div b and/or a modular reduction of a type r = a mod b is performed, where q is a quotient, a is a number containing m bits, b is a number containing n bits, with n less than or equal to m and b_{n-1} is non-zero, b_{n-1} being the most significant bit of the number b." Applicant respectfully disagrees.

First, paragraph [0004] in Drexler merely states that methods are known that allow a person monitoring the current consumption or timing of the encryption process to deduce secret data, in particular, a secret key. Nothing in paragraph [0004] in Drexler reads on Applicant's claims; rather, Applicant's claims solve this problem. Second, paragraph [0007] in Drexler discloses that it is known for a factor r*n (random number * modulus) to be added for the encryption of the message. The encrypted text $Y=M^d$ mod n is thus changed to $(M+r*n)^d$ mod n, where M is a known message.

However, even if paragraphs [0004] and [0007] in Drexler are combined, the resulting combination is still not the claimed embodiment. Moreover, the Examiner has not carried the burden of proving anticipation because the rejection lacks the specificity required under 35 U.S.C. § 102 to establish that these sections of Drexler teach every element of the claim arranged or combined in the same way as recited in the claim.

Next, paragraph [0020] in Drexler is cited for allegedly disclosing the claimed "masking the number a by a random number ρ before performing the integer division and/or the modular reduction." Applicant respectfully disagrees. In Applicant's claim where r = a mod b, where b is the modulus, number a is masked by a random number ρ before performing the integer division and/or the modular reduction. In contrast, as noted in paragraph [0020] in Drexler, random number r is multiplied by the modulus n. Thus, Drexler similarly fails to teach or suggest this element of claim 1 arranged or combined in the same way as recited in the claim.

Paragraph [0005] in Drexler is cited as allegedly disclosing the claimed "generating encrypted or decrypted data in accordance with a result of the division and/or modular reduction" (emphasis added). Applicant again respectfully disagrees.

Paragraph [0005] in Drexler discloses a type of attack ("Simple Power Analysis" (SPA) method), where the encrypted text $Y=M^d$ mod n is formed. During the modular exponentiation process, a squaring operation is carried out with the intermediate result and a multiplication operation is carried out with M if there is a "1" in the exponent d, while only a squaring operation with the intermediate result is carried out if there is a "0" in d. If M is known, the times at which the message M is used can be identified by observing the current response and/or the timing during the operations. Since this message is always used if a "1" is present in d, the key can be deduced without any problems.

However, since the claimed division and/or modular reduction is arrived at by masking the number a by a random number ρ before performing the integer division and/or the modular reduction, and since paragraph [0005] is Drexler does not teach or suggest this feature, the rejection of claim 1 should be withdrawn for this reason as well. Accordingly, Drexler fails to disclose every element of claim 1 arranged or combined in the same way as recited in the claim. Thus, claim 1 is allowable. This logic also disposes of the rejection of claims 2 and 5-8, which depend from claim 1.

Rejection Under 35 U.S.C. § 103

Claims 3 and 4 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Drexler and Falk U.S. Patent No. 5,077,793. Applicant also respectfully traverses this rejection. Claims 3 and 4 depend directly or indirectly from claim 1 and recite further distinguishing features and are thus also allowable because Drexler is cited for teachings it does not provide. Additionally, Falk, which is cited only for the use of modular subtractors to subtract pseudo-random number sequences from a converted encrypted signal, does not cure the deficiencies of Drexler.

Conclusion

For the foregoing reasons, Applicant respectfully submits that this application is in condition for allowance and all pending claims are patentably distinct from the cited references. Reconsideration and allowance of all pending claims, or, in the alternative, reopening prosecution, are respectfully requested. If additional fees are required for any reason, please charge Deposit Account No. 02-4800 the necessary amount.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: March 2, 2008

By: /Brian N. Fletcher/
Brian N. Fletcher
Registration No. 51683

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620
Customer No. 21839